WHAT IS CLAIMED IS:

1. A fingerprint authentication method comprising:

a first step of collating features of input data based on a fingerprint input by an user with features of enrolled data;

a second step of judging whether the input data are proper for authentication or not; and

a third step of authenticating the input data according to results of said first step and said second step; wherein

said second step is done by the use of a spatial frequency analysis of an input image represented by the input data.

2. A fingerprint authentication method as claimed in Claim 1, wherein said second step comprises:

a forth step of deciding a rectangular observation area on the input image;

a fifth step of finding Fourier transformed image from the input image;

a sixth step of calculating discriminative values on the basis of the Fourier transformed image, said discriminative values representing features of the spatial frequency distribution of brightness of the input image; and

a seventh step of deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

3. A fingerprint authentication method as claimed in Claim 2, wherein said seventh step is done by the use of one or more discriminants and corresponding discriminative coefficients which are previously calculated.

4. A fingerprint authentication method as claimed in

Claim 2, wherein said forth step comprises:

an eighth step of finding a fingerprint center and a fingertip direction on the input image; and

a ninth step of assuming the rectangular observation area on the input image on the basis of the fingerprint center and the fingertip direction.

5. A fingerprint authentication method as claimed in Claim 2, wherein said six step is done by the use of an average of strength values corresponding to a predetermined spatial frequency band in the Fourier transformed image.

6. A fingerprint authentication method as claimed in Claim 5, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of ridges of a human fingerprint.

7. A fingerprint authentication method as claimed in Claim 5, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of a periodic structure caused by sweat glands of a human finger.

8. A fingerprint authentication method as claimed in Claim 2, wherein said six step is done by the use of dispersion of strength values corresponding to a predetermined spatial frequency band in the Fourier transformed image.

9. A fingerprint authentication method as claimed in Claim 8, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of ridges of a human fingerprint.

10. A fingerprint authentication method as claimed in Claim 8, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period

of a periodic structure caused by sweat glands of a human finger.

11. A fingerprint authentication method as claimed in Claim 2, further comprising:

a tenth step of requesting the user to input the fingerprint once more when decision that the input data are not proper is made at said seventh step.

12. A computer readable program for making a computer system serve as a finger authentication device, comprising:

a first step of collating features of input data based on a fingerprint input by an user with features of enrolled data;

a second step of judging whether the input data are proper for authentication or not; and

a third step of authenticating the input data according to results of said first step and said second step; wherein

said second step is done by the use of a spatial frequency analysis of an input image represented by the input data.

13. A computer readable program as claimed in Claim 12, wherein said second step comprises:

a forth step of deciding a rectangular observation area on the input image;

a fifth step of finding Fourier transformed image from the input image;

a sixth step of calculating discriminative values on the basis of the Fourier transformed image, said discriminative values representing features of the spatial frequency distribution of the brightness of the input image; and

a seventh step of deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

14. A computer readable program as claimed in Claim 13, wherein said seventh step is done by the use of one or more discriminants and corresponding discriminative coefficients which are previously calculated.

15. A computer readable program as claimed in Claim 13, wherein said forth step comprises:

an eighth step of finding a fingerprint center and a fingertip direction on the input image; and

a ninth step of assuming the rectangular observation area on the input image on the basis of the fingerprint center and the fingertip direction.

16. A computer readable program as claimed in Claim 13, wherein said six step is done by the use of an average of strength values corresponding to a predetermined spatial frequency band in the Fourier transformed image.

17. A computer readable program as claimed in Claim 16, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of ridges of a human fingerprint.

18. A computer readable program as claimed in Claim 16, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of a periodic structure caused by sweat glands of a human finger.

19. A computer readable program as claimed in Claim 13, wherein said six step is done by the use of dispersion of strength values corresponding to a predetermined spatial frequency band in the Fourier transformed image.

20. A computer readable program as claimed in Claim 19, wherein said predetermined spatial frequency band includes a

spatial frequency corresponding to a generic period of ridges of a human fingerprint.

21. A computer readable program as claimed in Claim 19, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of a periodic structure caused by sweat glands of a human finger.

22. A computer readable program as claimed in Claim 13, further comprising:

a tenth step of requesting the user to input the fingerprint once more when decision that the input data are not proper is made at said seventh step.

23. A fingerprint authentication device comprising:

a collating portion for collating features of input data based on a fingerprint input by an user with features of enrolled data;

a characteristic judging portion for judging whether the input data are proper for authentication or not; and

a authenticating portion for authenticating the input data according to outputs from said collation portion and said characteristic judging portion; wherein

said characteristic judging portion uses a spatial frequency analysis of an input image represented by the input data to judge whether the input data are proper for authentication or not.

24. A fingerprint authentication device as claimed in Claim 23, wherein said characteristic judging portion comprises:

an observation area deciding portion for deciding a observation area on the input image;

a frequency analyzing portion for transforming image of the observation area into a Fourier transformed image;

a discriminative value calculating portion for calculating discriminative values on the basis of the Fourier transformed image, said discriminative values representing features of the spatial frequency distribution of brightness of the input image; and

a deciding portion for deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

25. A fingerprint authentication device as claimed in Claim 24, further comprises a discriminative coefficient holding portion for holding one or more discriminants and corresponding discriminative coefficients which are previously calculated by the use of said discriminants, wherein

said deciding portion uses said discriminants and said discriminative coefficients together with the discriminative values to decide whether the input data are proper for the authentication or not.

26. A fingerprint authentication device as claimed in Claim 24, wherein said observation line deciding portion executes of the steps of:

finding a fingerprint center and a fingertip direction on the input image; and

assuming the observation area on the input image on the basis of the fingerprint center and the fingertip dierection.

27. A fingerprint authentication device as claimed in Claim 24, wherein said discriminative value calculating portion uses an average of strength values corresponding to a predetermined spatial frequency band in the Fourier transformed

image.

28. A fingerprint authentication device as claimed in Claim 27, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of ridges of a human fingerprint.

29. A fingerprint authentication device as claimed in Claim 27, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of a periodic structure caused by sweat glands of a human finger.

30. A fingerprint authentication device as claimed in Claim 24, wherein said discriminative value calculating portion uses dispersion of strength values corresponding to a predetermined spatial frequency band in the Fourier transformed image.

31. A fingerprint authentication device as claimed in Claim 30, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of ridges of a human fingerprint.

32. A finger print authentication device as claimed in Claim 30, wherein said predetermined spatial frequency band includes a spatial frequency corresponding to a generic period of a periodic structure caused by sweat glands of a human finger.

33. A fingerprint authentication device as claimed in Claim 24, wherein said authenticating portion requests the user to input the fingerprint once more when the input data are not proper.